ON THE GROUP OF AUTOMATIC ONE-TO-ONE MAPPINGS

1964

SovietRxiv

Abstract

Full Text

V. P. ZAROVNY

ON THE GROUP OF AUTOMATIC ONE-TO-ONE MAPPINGS

(Presented by Academician A. I. Mal' tsev, 27 I 1964)

In the work of J. Hořejš ([1]) there was posed (as far as we know, for the first time) the problem of studying various classically expressible properties of the group of one-to-one mappings of the set of words in a finite alphabet onto itself, induced by finite automata. Below some results in this direction are set forth.

1. A **Mealy automaton** (see ([2])) is a collection $A = A(\mathfrak{A}, \mathfrak{X}, \mathfrak{Y}, \delta, \lambda, a_0)$ of six mathematical objects, of which $\mathfrak{A}, \mathfrak{X}, \mathfrak{Y}$ are sets, called respectively the **sets of states, inputs, and outputs**; δ is a function mapping $\mathfrak{A} \times \mathfrak{X}$ into $\mathfrak{A}$ and called the **transition function**; λ is a function mapping $\mathfrak{A} \times \mathfrak{X}$ into $\mathfrak{Y}$ and called the **output function**; a_0 is a fixed element of $\mathfrak{A}$, called the **initial state**. The **mapping induced by the automaton** A is the mapping φ_A of the set $F(\mathfrak{X})$ of words in the alphabet $\mathfrak{X}$ into the set $F(\mathfrak{Y})$ of words in the alphabet $\mathfrak{Y}$, defined by the condition

$$\varphi_A(x_{i_1} \dots x_{i_k}) = \lambda(a_0, x_{i_1})\lambda(a_0 x_{i_1}, x_{i_2}) \dots \lambda(a_0 x_{i_1} \dots x_{i_{k-1}}, x_{i_k}),$$

where $a_0 x$ denotes $\delta(a_0, x)$ and
$a_0 xy = \delta(a_0, xy) = \delta[\delta(a_0, x), y]$ for arbitrary $x, y \in \mathfrak{X}$.

The sets $\mathfrak{X}$ and $\mathfrak{Y}$ are always assumed finite. The automaton A is called **finite** if the set $\mathfrak{A}$ is also finite.

The definition of a Moore automaton is obtained by replacing, in the definition of a Mealy automaton, the function λ by the marking function $\mu : \mathfrak{A} \to \mathfrak{Y}$ and the condition for φ_A by the condition

$$\varphi_A(x_{i_1} \dots x_{i_k}) = \mu(a_0 x_{i_1})\mu(a_0 x_{i_1} x_{i_2}) \dots \mu(a_0 x_{i_1} \dots x_{i_k}).$$

It is known (see ([2]), p. 53) that the set of mappings induced by Mealy automata (finite Mealy automata) coincides with the set of mappings induced by Moore automata (finite Moore automata). This gives us grounds for using the term "automatic (respectively, finite-automatic) mapping."

Let now $\mathfrak{X} = (x_1, \dots, x_n)$ and $\mathfrak{Y} = \mathfrak{X}$. Denote by $F(n)$ the set of words in the alphabet $\mathfrak{X}$ of n letters; by $A(n)$ ($K(n)$), the set of all automatic (finite-automatic) one-to-one mappings of the set $F(n)$ onto itself; by $F(n, r)$, the

set of words of length r in an alphabet of n letters. We shall also introduce the notation l^p for the initial segment of length l of the word p. A mapping preserving the lengths of words will be called **isometric**.

2. On the basis of the obvious equalities

$$F(n) = \bigcup_{r=1}^{\infty} F(n, r)$$

and

$$F(n, i) \cap F(n, j) = \emptyset, \qquad i \neq j,$$

one can prove

Proposition 1. *The set $I(n)$ of one-to-one isometric mappings of the set $F(n)$ onto itself forms a group with respect to multiplication of mappings. This group is isomorphic to the complete direct*

direct product (see (4)) $\prod_{r=1}^{\infty} S_{n^r}$ of symmetric groups of degrees n^r, $r = 1, 2, \ldots$.

Using the criterion for automaticity of an alphabet mapping (see (3)), in particular the fact that alphabet mappings are isometric, we obtain, as a consequence of Proposition 1,

Proposition 2. There is an inclusion $A(n) \subseteq I(n)$, or, in other words, automatic one-to-one mappings of the set $F(n)$ onto itself can be specified by sequences of the form $\varphi = (\varphi_1, \ldots, \varphi_r, \ldots)$ of substitutions of the sets $F(n, 1), \ldots, F(n, r), \ldots$, and multiplied componentwise.

3. Automatic one-to-one mappings of the set $F(n)$ onto itself among isometric one-to-one mappings can be characterized by the following proposition:

Proposition 3. If $\varphi \in I(n)$ and $\varphi = (\varphi_1, \ldots, \varphi_r, \ldots)$ is its representation by the substitutions of the sets $F(n, 1), \ldots, F(n, r), \ldots$ induced by it, then the following assertions are equivalent:

a) φ is an automatic mapping;

b) for every $r = 1, 2, \ldots$ and every word $p \in F(n, r)$, for $1 \leq l \leq r$, the equality

$$_l[\varphi_r(p)] = \varphi_l({}_l p)$$

holds;

c) for every $r = 1, 2, \ldots$ and every word $p \in F(n, r)$, the equality

$$_{r-1}[\varphi_n(p)] = \varphi_{n-1}({}_{r-1} p).$$

The proof of this proposition is based on the criterion for automaticity of a mapping from (3). Using Proposition 3, one can prove the following theorem:

Theorem 1. The set $A(n)$ of all one-to-one automatic mappings of the set $F(n)$ onto itself is a group—a subgroup of $I(n)$.

This theorem is analogous to the fact proved by J. Hořejš in [1]. The set $K(n)$ of finite-automaton one-to-one mappings of the set $F(n)$ onto itself is a group.

Hence

Corollary 1. The set $K(n)$ is a subgroup of the group $A(n)$, and therefore also of the group $I(n)$.

4. For the study of the groups $A(n)$ and $K(n)$, the following concept turns out to be useful. A substitution of the set $F(n, r)$ is called **automatic** (**finite-automatic**) if it serves as the r-th component of at least one automatic (finite-automatic) and one-to-one mapping. We immediately obtain

Proposition 4. The set $A(n, r)$ (respectively $K(n, r)$) of automatic (finite-automatic) substitutions of the set $F(n, r)$ forms a group (a subgroup of the symmetric group S_{n^r}) with respect to multiplication of substitutions.

It is clear that $K(n, r) \subseteq A(n, r)$.

The use of the groups $A(n, r)$ and $K(n, r)$ for the study of the groups $A(n)$ and $K(n)$ is based on the following fact:

Proposition 5. The group $A(n)$ (the group $K(n)$) is a subdirect product (see (4)) of the groups $A(n, r)$ (the groups $K(n, r)$), $r = 1, 2, \ldots$.

In this connection there arises the problem of characterizing automatic (finite-automatic) substitutions. This problem is solved by

Proposition 6. In order that a substitution φ_r of the set $F(n, r)$ be automatic, it is necessary and sufficient that the following three requirements be satisfied (for any $p, q \in F(n, r)$, $1 \leq l \leq r$):

AP. 1. If ${}_lp = {}_lq$, then also ${}_l[\varphi_r(p)] = {}_l[\varphi_r(q)]$.

AP. 2. If ${}_l[\varphi_r(p)] = {}_l[\varphi_r(q)]$, then also ${}_lp = {}_lq$.

AP. 3. $F(n, l) = \{\, {}_l[\varphi_r(p)];\ p \in F(n, r)\,\}$.

Every automaton permutation is also finite-automaton, so that $A(n, r) = K(n, r)$ for any $r = 1, 2, \ldots$.

The necessity of conditions AP. 1-3 follows directly from Proposition 3 and the definition of an automaton permutation. To prove sufficiency, for $l < r$ and $k > r$ one considers the mappings associated with the permutation φ_r ($p \in F(n, l)$, $q \in F(n, k)$): $\varphi_{l/r}(p) = {}_l[(\varphi_r(px_{i_{l+1}} \ldots x_{i_r})]$, where $x_{i_{l+1}}, \ldots, x_{i_r}$ are arbitrary letters; $\varphi_{r/k}(q) = \varphi_{r/k}(x_{i_1} \ldots x_{i_r} x_{i_{r+1}} \ldots x_{i_k}) = \varphi_r(x_{i_1} \ldots x_{i_r}) x_{i_{r+1}} \ldots x_{i_k}$.

The meaning of conditions AP. 1-3 is that they ensure that $\varphi_{l/r}$ and $\varphi_{r/k}$ are permutations of the sets $F(n,l)$ and $F(n,r)$, respectively. The mapping

$$\varphi = (\varphi_{1/r}, \varphi_{2/r}, \dots, \varphi_{r-1/r}, \varphi_r, \varphi_{r/r+1}, \dots)$$

is considered, and it is proved that there exists a finite automaton inducing φ (whence it follows that if the permutation φ_r satisfies conditions AP. 1-3, then it is not only automaton, but also finite-automaton).

This automaton is constructed as follows. Its states are the symbols $a_\emptyset$ (the initial state), $a_{i_1 \dots i_k}$ ($i_1, \dots, i_k$ are natural numbers from the set $1, \dots, n$), a_*. The transition and output functions are given by the conditions:

$$a_\emptyset x_i = a_i; \qquad a_* x_i = a_*; \qquad a_{i_1 \dots i_k} x_{i_{k+1}} = \begin{cases} a_{i_1 \dots i_k i_{k+1}}, & \text{if } k \le r-1, \\ a_*, & \text{if } k > r-1; \end{cases}$$

$$\lambda(a_\emptyset x_i) = \varphi(x_i), \qquad \lambda(a_* x_i) = x_i; \qquad \lambda(a_{i_1 \dots i_k}, x_{i_{k+1}}) = \pi\varphi(x_{i_1} \dots x_{i_k} x_{i_{k+1}}),$$

where πp denotes the last letter of the word p.

If φ_r is an automaton permutation, then, by the first part of the proof, it satisfies conditions AP. 1-3, and by what was proved in the second part in this case it is finite-automaton, i.e. $A(n,r) \subseteq K(n,r)$, that is, $A(n,r) = K(n,r)$.

Taking this into account, one can, in particular, rephrase Proposition 5:

Proposition 5′. *Both the group $A(n)$ and the group $K(n)$ are direct products of the groups $K(n,r)$, $r = 1, 2, \dots$.*

5. It is known what importance knowledge of the order of a finite group has for the study of it. It is therefore important to compute the order $\rho[K(n,r)]$ of the group $K(n,r)$.

Theorem 2. *The order of the group $K(n,r)$ is expressed by the formula*

$$\rho[K(n,r)] = (n!)^{\frac{n^r-1}{n-1}}.$$

The proof is based on two lemmas.

Lemma 1. *There exists a homomorphism of the group $K(n,r)$ onto the group $K(n,r-1)$; as such a homomorphism one may take $\omega_{r-1/r} : \varphi_r \to \varphi_{r-1/r}$.*

Lemma 2. *The kernel of the homomorphism $\omega_{r-1/r}$ has order $(n!)^{n^{r-1}}$.*

After the proof of the lemmas, the proof of the theorem proceeds as follows: the index of the kernel of the homomorphism $\omega_{r-1/r}$ in $K(n,r)$ is equal to $\rho[K(n,r-1)]$, while its order is $(n!)^{n^{r-1}}$, so that

$$\rho[K(n,r)] = \rho[K(n,r-1)](n!)^{n^{r-1}},$$

whence, taking into account that $K(n,1) = S_n$, i.e.

$$\rho[K(n,1)] = n!,$$

we obtain

$$\rho[K(n,r)] = (n!)(n!)^{n^2-1} \dots (n!)^{r-1} = (n!)^{\sum_{i=1}^{r} n^{i-1}} = (n!)^{\frac{n^r-1}{n-1}}.$$

Using Theorem 2, we compute $p[K(2,2)] = 2^3 = 8$, after which it is not difficult to write out explicitly all the elements of the group $K(2,2)$, construct its Cayley table, and discover that six of its elements have order 2, two elements have order 4, and therefore the whole group is not cyclic; the least number of its generators is two.

Using this, one can obtain in a few words, in the following way, the proof of J. Hořejš' s theorem on the noncyclicity of $K(n)$: if $K(n)$ were cyclic, then the homomorphic image $K(n,r)$, for any n, r, would be a cyclic group (see Proposition 5). But for $n = 2$ the group $K(n,2)$, as noted, is not cyclic, while for $n > 2$ the group $K(n,1)$ is not cyclic.

It is interesting that, literally in the same words, on the basis of Proposition 5, one proves

Theorem 3. *The group $A(n)$ is not cyclic for any $n \geqslant 2$.*

6. Finally, one can prove that the group $K(n)$ satisfies neither the minimality condition nor the maximality condition.

Let $t = (i_1, \dots, i_k)$ (or $t = (i_1, \dots, i_k, \dots)$) be a strictly increasing finite (or infinite) sequence of nonzero natural numbers. A mapping φ from $K(n)$ is called a **mapping of type** t if in every word it leaves unchanged all letters standing in the positions numbered by the numbers from t.

Proposition 7. *The set $K(n)[t]$ of all mappings of type t is a subgroup of the group $K(n)$.*

Lemma 3. *The group $K(n)(r+1, \dots)$ is isomorphic to the group $K(n,r)$ for every r.*

Lemma 4. *The subgroup $K(n)(1, \dots, r)$ of the group $K(n)$ is the kernel of the homomorphism of the group $K(n)$ onto the group $K(n,r)$, i.e. a normal divisor of index $p[K(n,r)]$.*

Obviously, if $t \subseteq t'$, then $K(n)[t] \supseteq K(n)[t']$. Hence, and from Theorem 2, according to which all the numbers $p[K(n,r)]$ for $r = 1, 2, \dots$ are distinct, we obtain

Proposition 8. *The increasing sequence of subgroups of the group $K(n)$*

$$K(n)[r+1, \dots] \subseteq K(n)[r+2, \dots] \subseteq \cdots \subseteq K(n)[r+s, \dots] \subseteq \cdots$$

does not terminate.

Proposition 9. *The decreasing sequence of subgroups of the group* $K(n)$

$$K(n)[1,\dots,r] \subseteq K(n)[1,\dots,r+1] \supseteq \cdots \supseteq K(n)[1,\dots,r+s] \supseteq \cdots$$

does not terminate.

Ivano-Frankovsk State Pedagogical Institute

Received
21 I 1964

CITED LITERATURE

1. J. Hořejš, *Problems of Cybernetics*, issue 9, 1963, p. 23.
2. V. M. Glushkov, *Synthesis of Digital Automata*, Moscow, 1962.
3. V. M. Glushkov, *Russian Mathematical Surveys*, **16**, issue 5 (101), 3 (1963).
4. A. G. Kurosh, *Lectures on General Algebra*, Moscow, 1961.

Note: Figure translations are in progress. See original paper for figures.